Amendments to the Specification

Please replace paragraph [0004] with the following amended paragraph:

[0004] In general, if we let $F(q^n)$ be a finite field, where q is a prime or a prime power, the degree of the filed is n and its order is q^n. A basis for the finite field is a set of n elements $b_0, b_1, \ldots$ [[b_{n-1}]] $\underline{b_{n-1}} \in F(q^n)$ such that every element A of the finite field can be represented uniquely as a linear combination of basis elements:

$$\underline{A = \sum_{i=0}^{n-1} a_i b_I} \qquad [[A = \sum_{i=0}^{n-1} a_i b_I]]$$

Please replace paragraph [0017] with the following amended paragraph:

[0017] Referring to FIG. 2, in a second embodiment each of the correspondents A and B have a respective public key aP represented in terms of basis β_1 and bP represented in terms of basis β_2. The first correspondent A transmits its public key aP to the server H which performs the basis conversion on the element to a representation basis β_2 and transmits this key [[$aP\beta_2$]] $\underline{aP_{\beta 2}}$ to the second correspondent B. The second correspondent B also transmits its public key [[$b_P\beta_2$]] $\underline{bP_{\beta 2}}$ to the server where a basis conversion is performed on the key to the basis β_1 of the first correspondent. The key $bP_{\beta 1}$ is forwarded to the first correspondent A. Each of the correspondents then compute a common key by combining its private key with the other correspondents received public key. Thus, A computes $abP_{\beta 1}$, and B computes $baP_{\beta 2}$.

Please replace paragraph [0019] with the following amended paragraph:

[0019] In a third embodiment, again it is assumed that the correspondents A and B operate in bases ~~β1 and β2~~ $\underline{\beta_1 \text{ and } \beta_2}$ respectively. The bases ~~β1 and β2~~ $\underline{\beta_1 \text{ and } \beta_2}$ may represent any basis. Furthermore, we define a field element α such that correspondent A represents the element α in terms of the ~~basis β1~~ $\underline{\text{basis } \beta_1}$, and correspondent B represents the field element α in terms of ~~basis β2~~ $\underline{\text{basis } \beta_2}$. The correspondents make use of a bit string that is a function of a sequence of traces of the field element as a shared secret to perform the certain cryptographic operations.

Please replace paragraph [0020] with the following amended paragraph:

[0020] In this embodiment if we let p be a prime and let $q=p^m$, where $m \geq 1$. Let F_q be the finite field having q elements and $[[Fq^n]]$ $\underline{F_q^n}$, the n-dimensional extension. The cyclic group G of $[[Fq^n]]$ $\underline{F_q^n}$ over $[[Fq]]$ $\underline{F_q}$ is generated by the mapping $\sigma(\alpha)=\alpha^q$, $\alpha \in [[Fq^n]]$ $\underline{F_q^n}$, and is of order n. We may then define the trace function of $[[Fq^n]]$ $\underline{F_q^n}$ over F_q as

$$\mathrm{Tr}\, F_q^n \mid_{Fq}(\alpha) = \sum_{\eta=0} \eta(\alpha) = \sum_{i=0}^{n-1} \alpha^{q^i}$$

Please replace paragraph [0021] with the following amended paragraph:

[0021] For brevity, the trace function is simply represented as Tr. The traces $Tr(\alpha_{\beta 1})$ and $Tr(\alpha_{\beta 2})$, have the property that the trace of an element α represented in terms of a basis $[[\beta 1]]$ $\underline{\beta_1}$ is the same as the trace of the element α represented in terms of basis $[[\beta 2]]$ $\underline{\beta_2}$.

Please replace paragraph [0023] with the following amended paragraph:

[0023] In general if $F(q^n)$ is the finite field and F(q) is the ground field over which it is defined, the elements of the finite field can be represented in a number of ways depending on the choice of basis. Two common types of basis are polynomial basis and normal basis. If [[β1]] $\underline{\beta_1}$ is a polynomial basis, then the basis elements may be represented as 1, β, β^2, ... β^{n-1}, where β is a root or generator. Assuming the function f(x)=0 and f(x) is an irreducible of degree n i.e irreducible over the ground field, then, if a field element is given by $\alpha = a_0+a_1\beta^1 \ldots + a_{n-1}\beta^{n-1}$, the trace is given by

$$Tr(a)= a_0+a_1Tr(\beta)+a_2Tr(\beta^2) \ldots + a_{n-1}Tr(\beta^{n-1}).$$

Please replace paragraph [0040] with the following amended paragraph:

[0040] Referring to FIG. 3, a key agreement scheme shows the correspondents A and B operating in bases [[β1 and β2]] $\underline{\beta_1 \text{ and } \beta_2}$ respectively. The bases [[β1 and β2]] $\underline{\beta_1 \text{ and } \beta_2}$ may represent any basis. Furthermore A and B each have the following system parameters, a long term private key d and a long-term public key $Q_A=d_aP$ and $Q_B=d_bP$, where P is a point on an elliptic curve represented in terms of the respective bases. The correspondent A represents P in terms of the basis [[β1]] $\underline{\beta_1}$ and correspondent B represents P in terms of basis [[β2]] $\underline{\beta_2}$. In a typical Diffie-Hellman key agreement scheme, each of the correspondents A and B generate respective ephemeral private keys k_A and k_B and compute a corresponding short term (session) public keys $k_AP_{\beta 1}$, and $k_BP_{\beta 2}$. A and B exchange their respective public keys, and convert them to their own basis. If the correspondents are low power devices, such as smart cards or the like, then basis conversion may be performed by an intermediate processor such as described with reference to FIGS. 1 and 2. Alternatively, if the correspondents have sufficient compiling power,

then basis conversion may be performed by the correspondents themselves, according to one of many basis conversion methods. In any event, after the basis conversion, correspondent A has B's public key $(k_\beta P_{\beta 2})_{\beta 1}$, and B has A's public key $(k_A P_{\beta 2})_{\beta 1}$. A shared secret is computed in their respective basis by computing $k_A(k_B P_{\beta 2})_{\beta 1} = \alpha_{\beta 1}$, and $k_B(k_A P_{\beta 1})_{\beta 2} = \alpha_{\beta 2}$. Each of the correspondents takes a sequence of traces of their respective field element α to derive a common bit string.

Please replace paragraph [0041] with the following amended paragraph:

[0041] Applying the method to a signature scheme, the correspondent A generates its ephemeral public session key $kP_{\beta 1}$. A trace sequence may be constructed, for example, of the x-coordinate of $kP_{\beta 1}$ producing a bit string T. The bit string is passed through a hash function g to derive a signature component r. A second signature component $s=k^{-1}(m+dr)$ is computed, where d is A's long term private key. The signature components are transmitted to B for verification. The verifier B computes $E'ms^{-1} P_{\beta 2} + rs^{-1} \underline{Q_{A_{\beta 2}}} [[Q_{A\beta 2}]] = kP_{\beta 2}$ where $\underline{Q_{A_{\beta 2}}} [[Q_{A\beta 2}]]$ is the long term public key of A in basis 2. This basis conversion could be performed by A using an intermediate H as described earlier. B then generates a sequence on the computed value $kP_{\beta 2}$, and applies the hash function g to derive a value r'. If r'=r, then the signature is verified.